REMARKS

The Final Office Action of October 8, 2010 and the Advisory Action of December 23, 2010 has been carefully reviewed. In response, Applicant hereby submits this Amendment and Response with RCE. Applicants submit that this paper and attached RCE conforms to the requirements of 37 CFR 1.114, and respectfully request the Examiner reconsider the rejections, and allow the pending claims in view of the following remarks.

Claims 1-23, 26, and 27 were pending. Claim 12 is hereby canceled. Claims 1, 13, 17, 26, and 27 are currently amended. Therefore, claims 1-11, 13-23, 26, and 27 are currently pending.

Rejected Claims

The Final Office Action rejected claims 1, 26, and 27 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 7,072,865 (Akiyama). Claims 2-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Akiyama in view U.S. Patent Application Publication 2005/0015583 (Sarkkinen). Claim 12 is hereby canceled. Claims 2-11 and 13-22 depend from claim 1. Therefore claims 1-11, 13-22, 26, and 27 stand or fall on the application of Akiyama to independent claims 1, 26, and 27. Claim 23 stands or falls on the application of the combination of Akiyama and Sarkkinen to claim 23.

Akiyama fails to anticipate claims 1-11, 13-22, 26, and 27 because Akiyama fails to teach 1) generating a broadcast key based upon a user identity key; 2) receiving multicast service activation data; and 3) sending from the user device the generated broadcast key. Claims 1, 26, and 27 read:

> 1. A multicast content accessing method for use on a user device, wherein a multicast service provides the multicast content, comprising:

> **receiving multicast service activation data** over a network;
>
> **generating on the user device a broadcast key based upon a user identity key**;
>
> **sending from the user device the generated broadcast key over a network**;
>
> wherein the generated broadcast key indicates that multicast content is to be provided to the user device.
>
> 26. A multicast content accessing apparatus for use on a user device, wherein a multicast service provides the multicast content, comprising:
>
> a data storage mechanism that stores a user identification key and **multicast service activation data**;
>
> key generation operation instructions configured to **generate on the user device a broadcast key based upon the stored user identification key** and the multicast service activation data;
>
> instructions configured to **send from the user device the generated broadcast key** over a network;
>
> wherein the generated broadcast key indicates that multicast content is to be provided to the user device.
>
> 27. A multicast content accessing apparatus for use on a user device, wherein a multicast service provides the multicast content, comprising:
>
> means for **receiving multicast service activation data** over a network;
>
> means for **generating on the user device a broadcast key based upon a user identification key**;
>
> means for **sending from the user device the generated broadcast key** over a network;
>
> wherein the generated broadcast key indicates that multicast content is to be provided to the user device.

(Emphasis added). As shown above, claims 1, 26, and 27 require 1) generating a broadcast key based upon a user identity key; 2) receiving multicast service activation data; and 3) sending from the user device the generated broadcast key. In contrast, Akiyama describes generating a response packet based on a secret key:

> If the challenge is a signature generation inquiry (step S113), the response generator 154 acquires a challenge information segment as data to be signed (step S121), **acquires a secret key** stored in a secret key storage 153 of the receiver apparatus (step S122), **and generates a signature** for the challenge information segment (step S123). **The generated signature is converted into the format of a response information** segment in accordance with the predetermined format, **and is sent in the form of a response packet to the center** (steps S123 to S125). If the challenge

> applies to none of the above three challenges, an error message is sent to the center (step S114).

Akiyama, col. 15, ll. 41-52 (emphasis added). As shown above, Akiyama's receiver acquires a secret key and generates a signature based on the secret key. A response packet containing a signature is not the same as a broadcast key. Even if the signature is interpreted as a broadcast key, the signature is based on a secret key, not a user identity key. Thus, Akiyama fails to teach generating a broadcast key based upon a user identity key.

Further in contrast to claims 1, 26, and 27, Akiyama fails to teach receiving multicast activation data:

> It is an object of the present invention to provide **a broadcast receiving method**, which can provide secure pay broadcast services, which can prevent wrong audience without pressing the broadcast band even when the number of subscribers increases, a broadcast receiving apparatus using the method, an information distributing method, and an information distributing apparatus using the distributing method.

Akiyama, col. 2, ll. 36-43 (emphasis added). As shown above, Akiyama is directed to a **broadcast** receiving method. Akiyama fails to disclose multicast communication. It is well known that a broadcast communication is directed to all subscribers, while a multicast communication is directed to multiple specific users. See for example [0032] of Applicant's published application. In addition, Newton's Telecom Dictionary describes multicast as a message sent to a 'selected' group. Thus, the broadcast method described by Akiyama, could not possibly be multicast activation data.

Still further in contrast to claims 1, 26, and 27, and as shown above, Akiyama's receiver sends the response packet containing the signature, not a generated broadcast key. Thus Akiyama fails to teach sending the generated broadcast key. As such, Akiyama fails to teach several elements of claims 1, 26, and 27, and consequently fails to anticipate claims 1-11, 13-22, 26, and 27.

Claim 23 contains elements similar to claim 1. Claim 1 is allowable in light of Akiyama for the reasons given above. Sarkkinen fails to remedy Akiyama's shortcomings, because Sarkkinen does not send ciphering information over the network from a user device. Therefore, the combination of Akiyama and Sarkkinen fails to teach an element of claim 23 and consequently fails to anticipate claim 23.

CONCLUSION

The Applicant respectfully submits that the Application, in its present form, is in condition for allowance. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Applicant intends this communication to be a complete response to the Final Office Action mailed October 8, 2010 and the Advisory Action mailed December 23, 2010.

The Commissioner is hereby authorized to charge payment of any fee associated with any of the foregoing papers submitted herewith or any fees during the prosecution of the present case to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,

CONLEY ROSE, P.C.

Date: 3-8-11

J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 750
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289